

SISTEM KEAMANAN RUANGAN BERBASIS *IoT* DENGAN AUTENTIKASI *RFID* DAN MONITORING AKSES MELALUI *WEB SERVER* DI LPM UNSIKA

Bhanu Azizi^{1*}, Purwantoro², Susilawati³

^{1,2,3}Informatika, Fakultas Ilmu Komputer; Universitas Singaperbangsa Karawang, Jl. HS. Ronggowaluyo, Telukjambe Timur, Karawang -41361, Telp/Fax: (0267) 641177

Keywords:

Internet of Things; RFID; ESP32; Automatic Door Lock; Web Server.

Correspondent Email:

2210631170013@student.unsika.ac.id

Abstrak. Keamanan ruangan merupakan aspek krusial dalam lingkungan organisasi kampus. Ruang Redaksi Lembaga Pers Mahasiswa (LPM) UNSIKA menyimpan berbagai aset penting, namun sistem kunci konvensional yang digunakan rentan terhadap risiko duplikasi dan keterbatasan kontrol akses individu. Penelitian ini merancang dan mengimplementasikan sistem kunci pintu otomatis berbasis *Internet of Things* (IoT) dengan autentikasi *RFID* terintegrasi *web server* untuk pemantauan akses secara *real-time*. Sistem dikembangkan menggunakan metode R&D model 4D (adaptasi tiga tahap) dengan komponen ESP32, RFID MFRC522, solenoid door lock, ESP32-CAM, LCD 16x2, buzzer, React JS, dan MySQL. Black Box Testing terhadap 16 skenario seluruhnya valid, dan User Acceptance Testing (UAT) terhadap 30 responden menghasilkan penerimaan 93,11% kategori Sangat Baik. Sistem mampu memverifikasi kartu *RFID* pada jarak 0–3 cm dengan rata-rata respons aktuasi 1,32 detik, serta mendokumentasikan setiap akses melalui foto otomatis ESP32-CAM yang tersimpan pada log *web server*.



Copyright © 2026 The Author(s), Published by Jurnal Informatika dan Teknik Elektro Terapan. This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Abstract. Room security is a crucial aspect in campus organizational environments. The Editorial Room of Lembaga Pers Mahasiswa (LPM) UNSIKA stores various important assets, yet its conventional lock system is vulnerable to duplication risks and limited individual access control. This study designs and implements an IoT-based automatic door lock system using RFID authentication integrated with a web server for real-time access monitoring. The system was developed using the R&D 4D model (adapted into three stages) with components consisting of ESP32, RFID MFRC522, solenoid door lock, ESP32-CAM, 16x2 LCD, buzzer, React JS, and MySQL. Black Box Testing across 16 scenarios were all valid, and User Acceptance Testing (UAT) involving 30 respondents yielded an acceptance rate of 93.11% categorized as Very Good. The system verified RFID cards within 0–3 cm with an average actuation response of 1.32 seconds, and documented every access activity through automatic photos stored in the web server log.

1. PENDAHULUAN

Keamanan fisik ruangan merupakan aspek krusial dalam setiap organisasi, termasuk di lingkungan kampus. Pengendalian akses fisik berfungsi untuk membatasi siapa saja yang

dapat memasuki suatu ruangan atau area tertentu yang menyimpan aset penting, sehingga menjadi fondasi perlindungan yang mengurangi risiko bagi organisasi [1]. Salah satu ruangan dengan kebutuhan keamanan

tinggi adalah Ruang Redaksi Lembaga Pers Mahasiswa (LPM) Universitas Singaperbangsa Karawang (UNSIKA), yang menyimpan berbagai arsip penting seperti naskah berita, dokumentasi kegiatan, alat rekam, dan peralatan redaksi lainnya. Selain itu, para wartawan kampus umumnya menggunakan nama samaran (*pseudonim*) untuk menjaga identitas dan independensi mereka, sehingga ruang ini memiliki tingkat kerahasiaan yang tinggi.

Sistem keamanan yang selama ini digunakan di ruang redaksi LPM UNSIKA masih berupa kunci manual konvensional. Kunci konvensional dinilai belum memadai untuk keamanan modern karena rentan terhadap risiko kehilangan, duplikasi tanpa izin, serta ketidakmampuan dalam mengontrol dan mencatat identitas individu yang mengakses ruangan [2]. Kondisi ini meningkatkan risiko kebocoran informasi maupun kehilangan aset penting organisasi.

Seiring perkembangan teknologi, penerapan *Internet of Things* (IoT) dalam bidang keamanan fisik ruangan semakin banyak digunakan. Universitas dan institusi pendidikan telah menggunakan perangkat IoT untuk keamanan fisik, termasuk penggunaan *RFID* untuk perekaman insiden secara real-time dan pengelolaan akses terpusat [3]. Salah satu teknologi yang banyak diimplementasikan dalam sistem kontrol akses berbasis IoT adalah *Radio Frequency Identification* (RFID), yang memungkinkan sistem mengenali identitas pengguna melalui kartu atau *tag* secara nirkontak [4].

Beberapa penelitian terdahulu telah mengembangkan sistem kontrol akses berbasis *RFID* dan IoT. Nurwijayanti dan Basyir [5] merancang sistem keamanan pintu otomatis menggunakan *NodeMCU ESP8266* dan *RFID RC522* yang mampu mengirimkan notifikasi melalui Telegram, namun belum dilengkapi *web server* atau sistem monitoring berbasis browser yang menyajikan data akses secara historis. Fathiah dkk. [6] mengembangkan *smart door lock* dengan autentikasi ganda *RFID* dan *keypad* untuk meningkatkan keamanan, namun sistem belum mendukung pemantauan jarak jauh maupun pencatatan aktivitas akses secara digital. Ramadini dan Hastuti [7] menghasilkan prototipe kunci pintu berbasis *RFID* yang mampu mencatat aktivitas akses

melalui jaringan IoT, namun belum menyediakan analisis data historis dan pelaporan terstruktur. Jardian dkk. [8] memanfaatkan *ESP32-WROVER* untuk kontrol pintu otomatis dengan notifikasi melalui aplikasi Blynk, namun tidak memiliki fitur autentikasi berlapis maupun penyimpanan data akses secara terpusat. Candra dan Elvantio [9] membangun sistem pembuka kunci pintu berbasis IoT dengan dokumentasi foto menggunakan *ESP32-CAM*, namun belum menyediakan fitur penyimpanan dan analisis data historis secara menyeluruh serta notifikasi *real-time* saat terjadi pelanggaran akses.

Berdasarkan kajian terhadap penelitian-penelitian tersebut, terdapat kesenjangan yang belum terpenuhi secara bersamaan, yaitu kombinasi antara autentikasi *RFID*, dokumentasi visual otomatis berbasis kamera, dan monitoring terpusat melalui *web server* dalam satu sistem terintegrasi. Penggunaan *RFID* saja masih memiliki keterbatasan dalam hal pembuktian visual apabila terjadi penyalahgunaan kartu oleh pihak yang tidak berhak [10]. Akbar dkk. [11] membuktikan bahwa integrasi IoT dengan *web server* berbasis *ESP32* mampu menyajikan data aktivitas secara *real-time*, namun belum mengintegrasikan dokumentasi visual sebagai bukti autentikasi sekunder.

Penelitian ini bertujuan merancang dan mengimplementasikan sistem keamanan kontrol akses fisik ruangan berbasis IoT pada Ruang Redaksi LPM UNSIKA, menggunakan autentikasi *RFID* yang dikombinasikan dengan kamera *ESP32-CAM* untuk dokumentasi visual otomatis, serta terintegrasi dengan *web server* sebagai platform monitoring dan manajemen akses secara *real-time*. Kebaruan penelitian ini terletak pada kombinasi dua keunggulan yang belum ditemukan secara bersamaan pada penelitian sebelumnya, yaitu histori penggunaan ruangan yang lengkap beserta bukti foto otomatis pada setiap aktivitas akses, serta kemampuan deteksi penyalahgunaan akses melalui dokumentasi visual yang memungkinkan administrator mengidentifikasi apakah kartu *RFID* digunakan oleh pemilik yang sah.

2. TINJAUAN PUSTAKA

2.1. *Internet of Things (IoT)*

Internet of Things (IoT) merupakan konsep teknologi yang menghubungkan berbagai perangkat elektronik agar dapat saling berkomunikasi dan bertukar data melalui jaringan internet [12]. *IoT* terdiri dari tiga komponen utama, yaitu input yang berfungsi mengumpulkan data dari lingkungan menggunakan sensor, proses yang mengolah data melalui mikrokontroler atau sistem tertanam, serta output yang mengeksekusi respons sesuai instruksi yang telah diproses [13]. Penerapan *IoT* banyak ditemukan pada berbagai bidang seperti industri, transportasi, kesehatan, hingga sistem keamanan modern.

2.2. *Radio Frequency Identification (RFID)*

RFID merupakan teknologi identifikasi otomatis yang menggunakan gelombang radio untuk mengenali dan melacak objek tanpa memerlukan kontak langsung [14]. *RFID* memiliki dua komponen utama, yaitu *tag* yang menyimpan nomor identifikasi unik (*UID*) pada chip berukuran sangat kecil, dan *reader* yang memancarkan gelombang radio untuk mendeteksi dan membaca *tag* dalam jangkauannya. Modul *MFRC522* merupakan *reader RFID* yang bekerja pada frekuensi 13,56 MHz dengan standar komunikasi ISO/IEC 14443A, memiliki jarak baca efektif 0–3 cm, dan berkomunikasi dengan mikrokontroler melalui antarmuka SPI [15].

2.3. *Mikrokontroler ESP32*

ESP32 merupakan mikrokontroler yang dikembangkan oleh Espressif Systems dengan arsitektur *dual-core Tensilica LX6* berkecepatan hingga 240 MHz, dilengkapi fitur *Wi-Fi 802.11 b/g/n*, *Bluetooth v4.2*, serta berbagai antarmuka komunikasi seperti *SPI*, *I²C*, dan *UART* [16]. Keunggulan *ESP32* terletak pada kemampuan pemrosesan yang cepat, konsumsi daya rendah, dan dukungan konektivitas ganda yang menjadikannya ideal untuk aplikasi *IoT* yang membutuhkan komunikasi nirkabel secara efisien.

2.4. *ESP32-CAM*

ESP32-CAM merupakan modul mikrokontroler berbasis *ESP32* yang dilengkapi kamera *OV2640* secara terintegrasi, mendukung konektivitas *Wi-Fi* dan *Bluetooth*

dengan konsumsi daya rendah, serta dilengkapi slot *MicroSD* untuk penyimpanan lokal [17]. Kemampuan pengambilan gambar secara *event-driven* menjadikan *ESP32-CAM* komponen yang tepat untuk sistem keamanan berbasis *IoT* yang membutuhkan fitur dokumentasi visual otomatis.

2.5. *Komponen Aktuator dan Indikator*

Solenoid door lock adalah aktuator elektromagnetik yang dirancang untuk mekanisme penguncian pintu elektronik, terdiri dari kumparan yang menghasilkan medan magnet saat dialiri tegangan listrik untuk menggerakkan plunger ke posisi terkunci atau terbuka [18]. Modul relay berfungsi sebagai saklar otomatis yang memungkinkan pengendalian sirkuit bertegangan tinggi (12V) menggunakan sinyal bertegangan rendah dari mikrokontroler [7]. LCD 16x2 dengan komunikasi *I²C* digunakan untuk menampilkan status akses kepada pengguna secara langsung, sedangkan *buzzer* berfungsi sebagai indikator suara yang memberikan notifikasi audio sesuai hasil autentikasi [19].

2.6. *Komponen Software*

Web server merupakan perangkat lunak yang menerima permintaan dari klien melalui protokol *HTTP*, memproses data yang diminta, dan mengirimkan hasilnya dalam bentuk halaman *web* [11]. MySQL merupakan sistem manajemen basis data yang efisien dan stabil, banyak digunakan dalam pengembangan aplikasi berbasis web karena mendukung penggunaan oleh banyak pengguna secara bersamaan menggunakan bahasa SQL [20]. Express.js merupakan framework web backend berbasis Node.js yang menyediakan struktur pengembangan aplikasi secara efisien melalui dukungan middleware untuk pengelolaan rute, parsing data, dan autentikasi [21]. React JS merupakan *library JavaScript open-source* untuk membangun antarmuka pengguna berbasis *single-page* dengan konsep reusable components yang mempercepat proses pengembangan [22].

2.7. *Metode Research and Development (R&D) Model 4D*

Metode *R&D* merupakan metode penelitian yang bertujuan menghasilkan produk baru atau memperbaiki produk yang telah ada agar lebih

efektif dan bermanfaat [23]. Model 4D yang dikembangkan oleh Thiagarajan, Semmel, dan Semmel terdiri dari empat tahap, yaitu *Define* (Pendefinisian), *Design* (Perancangan), *Develop* (Pengembangan), dan *Disseminate* (Penyebaran) [24]. Dalam penelitian ini, model 4D diadaptasi menjadi tiga tahap dengan menghilangkan tahap *Disseminate* sesuai ruang lingkup penelitian tingkat Strata Satu.

2.8. Black Box Testing

Black Box Testing merupakan metode pengujian perangkat lunak yang berfokus pada pengujian fungsionalitas sistem tanpa memperhatikan struktur internal atau logika program [25]. Penguji hanya menilai apakah keluaran yang dihasilkan sesuai dengan masukan yang diberikan berdasarkan spesifikasi yang telah ditetapkan, bertujuan untuk memastikan sistem berfungsi dengan benar dari sudut pandang pengguna.

2.9. User Acceptance Testing (UAT)

User Acceptance Testing (UAT) merupakan tahap pengujian yang bertujuan menilai sejauh mana sistem dapat diterima dan memenuhi kebutuhan operasional pengguna secara nyata [26]. Penilaian dilakukan menggunakan kuesioner berbasis Skala Likert dengan lima pilihan jawaban berskor 1–5 seperti ditunjukkan pada Tabel 1. Hasil perhitungan persentase penerimaan menggunakan rumus pada Persamaan (1) [27].

$$\frac{\sum \text{Skor yang Diperoleh}}{\sum \text{Skor Maksimum}} \times 100\% \quad (1)$$

Keterangan: P = persentase penerimaan pengguna. Interpretasi hasil *UAT* menggunakan kategori persentase seperti ditunjukkan pada Tabel 2 [26]. Penentuan jumlah responden mengacu pada Nielsen (2000) yang menyatakan bahwa pengujian dengan 5 pengguna sudah cukup untuk menemukan permasalahan yang hampir sama banyaknya dibandingkan menggunakan lebih banyak responden [28].

Tabel 1. Skala Likert

Pilihan Jawaban	Skor
Sangat Setuju	5
Setuju	4
Netral	3
Tidak Setuju	2

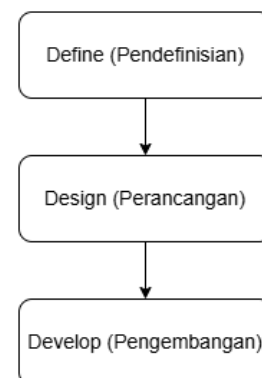
Sangat Tidak Setuju 1

Tabel 2. Interpretasi Persentase UAT

Skor	Keterangan
$0\% \leq x < 36\%$	Tidak Baik
$36\% < x < 52\%$	Kurang Baik
$52\% < x < 68\%$	Netral
$68\% < x < 84\%$	Baik
$84\% < x < 100\%$	Sangat Baik

3. METODE PENELITIAN

Penelitian ini menggunakan metode *Research and Development* (R&D) dengan model pengembangan *Four-D* (4D) yang diadaptasi menjadi tiga tahap, yaitu *Define*, *Design*, dan *Develop*. Pembatasan ini dilakukan karena titik berat penelitian terletak pada perancangan fungsional dan pengujian teknis sistem secara langsung di Ruang Redaksi LPM UNSIKA, tanpa mencakup tahap penyebaran produk secara lebih luas. Alur tahapan penelitian ditunjukkan pada Gambar 1.



Gambar 1. Rancangan Penelitian

3.1. Define (Pendefinisian)

Tahap *Define* merupakan tahap awal yang bertujuan mengidentifikasi permasalahan, menganalisis kebutuhan pengguna, serta merumuskan tujuan pengembangan sistem melalui lima langkah berikut.

3.1.1. Front-end Analysis

Dilakukan melalui observasi langsung dan wawancara dengan pengurus inti LPM UNSIKA. Hasil analisis menemukan bahwa sistem keamanan yang berjalan masih menggunakan kunci manual yang dipegang bersama oleh beberapa pengurus, sehingga menimbulkan risiko kehilangan kunci, sulitnya mengontrol identitas pengguna yang mengakses

ruangan, serta tidak adanya pencatatan aktivitas akses secara otomatis.

3.1.2. User Analysis

Pengguna sistem terdiri dari dua kelompok utama: (1) anggota aktif LPM UNSIKA sebagai pengguna fisik yang berinteraksi langsung melalui pemindaian kartu RFID, dan (2) pengurus inti LPM UNSIKA sebagai administrator yang mengelola data dan memantau sistem melalui antarmuka web server. Karena seluruh pengguna berlatar belakang non-teknis, sistem dirancang agar mudah dioperasikan tanpa pelatihan khusus.

3.1.3. Task Analysis

Berdasarkan analisis kebutuhan keamanan fisik ruangan, dirumuskan lima fungsi utama yang harus diimplementasikan:

1. Autentikasi identitas pengguna secara unik melalui kartu *RFID*
2. Dokumentasi visual otomatis melalui kamera pada setiap aktivitas akses
3. Peringatan langsung melalui *LCD* dan *buzzer* saat terdeteksi akses tidak terdaftar
4. Perekaman seluruh riwayat aktivitas akses beserta foto ke dalam basis data
5. Pemantauan terpusat melalui antarmuka web secara *real-time*.

3.1.4. Concept Analysis

Konsep utama yang diangkat sebagai solusi adalah *IoT* karena kemampuannya mengintegrasikan pengendalian perangkat keras secara fisik dengan server melalui jaringan nirkabel. Tiga konsep pendukung diterapkan: identifikasi nirkontak berbasis *RFID* sebagai mekanisme autentikasi, dokumentasi visual terintegrasi menggunakan kamera mikrokontroler sebagai autentikasi sekunder, serta pemantauan berbasis *web* sebagai pusat kendali administrator.

3.1.5. Specifying System Objectives

Tujuan akhir sistem dirumuskan sebagai berikut:

1. Membangun sistem kunci pintu otomatis berbasis *IoT* menggunakan ESP32 dan RFID MFRC522
2. Mengintegrasikan ESP32-CAM sebagai fitur dokumentasi visual *event-driven*
3. Mengembangkan antarmuka monitoring berbasis web untuk pemantauan *real-time*

4. menghasilkan sistem terintegrasi yang andal dan mudah dioperasikan oleh pengguna non-teknis.

3.2. Design (Perancangan)

Tahap *Design* berfungsi mengubah hasil analisis kebutuhan menjadi rancangan sistematis yang siap diimplementasikan melalui empat langkah berikut.

3.2.1. Constructing Criterion-Referenced Test

Instrumen pengujian dirancang menggunakan metode *Black Box Testing* yang berfokus pada akurasi pembacaan *UID* oleh sensor *RFID*, kesesuaian respons aktuasi *solenoid door lock*, keberhasilan kamera dalam menangkap gambar secara *event-driven*, serta kesesuaian data riwayat akses yang dikirim dan ditampilkan pada antarmuka *web server*.

3.2.2. Media Selection

Perangkat keras dirancang menggunakan arsitektur dual-microcontroller, di mana ESP32 bertindak sebagai pengontrol utama untuk memproses input dari modul RFID MFRC522, mengendalikan aktuator solenoid door lock 12V via modul relay, serta memberikan output melalui LCD 16x2 dan buzzer; sedangkan ESP32-CAM bertindak sebagai pengontrol sekunder khusus untuk fungsi dokumentasi visual. Perangkat lunak menggunakan Arduino IDE untuk pemrograman mikrokontroler, MySQL untuk basis data, serta Node.js, Express JS, dan React JS untuk sistem backend dan frontend web server.

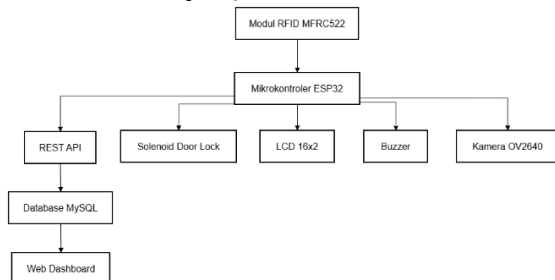
3.2.3. Format Selection

Perangkat keras dirakit dalam bentuk prototype di dalam box akrilik dan dipasang langsung pada pintu Ruang Redaksi LPM UNSIKA. Perangkat lunak mengadaptasi arsitektur client-server terpusat dengan dua level hak akses: Administrator dengan akses penuh (CRUD) untuk mengelola data kartu RFID dan akun pengguna, serta Viewer dengan akses read-only untuk memantau log aktivitas akses.

3.2.4. Initial Design

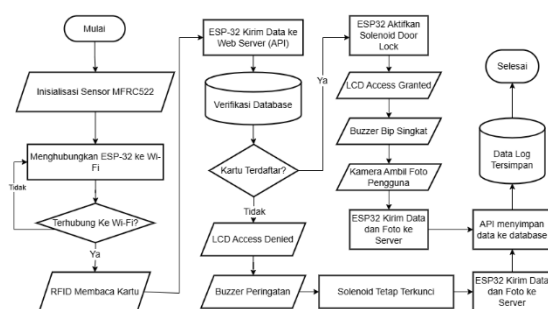
Rancangan awal divisualisasikan melalui Diagram Blok Sistem dan Flowchart Sistem. Berdasarkan Gambar 2, sistem menggunakan arsitektur dual-microcontroller di mana ESP32

menerima input *UID* dari *RFID MFRC522*, mengendalikan *solenoid door lock* melalui modul relay, serta memberikan output melalui *LCD* dan *buzzer*. *ESP32-CAM* terhubung dengan kamera *OV2640* untuk dokumentasi visual. Kedua mikrokontroler mengirimkan data ke *web server* secara nirkabel melalui protokol *HTTP*, yang kemudian memproses logika verifikasi dan menyimpan riwayat akses ke basis data *MySQL*.



Gambar 2. Diagram Blok Sistem

Berdasarkan Gambar 3, alur kerja sistem dimulai dengan inisialisasi jaringan. Ketika kartu didekatkan, sensor *RFID* membaca *UID* dan mengirimkannya ke server untuk dicocokkan dengan basis data. Jika *UID* valid, sistem mengaktifkan relay sehingga pintu terbuka, membunyikan *buzzer* (dua bip pendek), menampilkan "Akses Diterima" pada *LCD*, dan menginstruksikan *ESP32-CAM* mengambil foto. Jika *UID* tidak terdaftar, sistem menolak akses, membunyikan *buzzer* (satu bip panjang), menampilkan "Akses Ditolak" pada *LCD*, dan tetap mengambil foto dokumentasi. Seluruh riwayat aktivitas dikirim ke server secara *real-time*.



Gambar 3. Flowchart Sistem

3.3. Develop (Pengembangan)

Tahap Develop merealisasikan rancangan menjadi produk nyata melalui dua proses utama.

3.3.1. Proses Development

Perakitan perangkat keras dilakukan dengan menyusun seluruh komponen elektronik di dalam box akrilik sebagai media mounting yang kemudian dipasang langsung pada pintu Ruang Redaksi LPM UNSIKA. Koneksi antarkomponen ditunjukkan pada Tabel 3 hingga Tabel 8.

Tabel 3. Koneksi *RFID MFRC522* dengan *ESP32*

MFRC522	ESP32
VCC	3.3V
GND	GND
SDA	21
SCK	18
MOSI	23
MISO	19
RST	22

Tabel 4. Koneksi *LCD 16x2 I2C* dengan *ESP32*

LCD I2C	ESP32
VCC	5V
GND	GND
SDA	21
SCL	22

Tabel 5. Koneksi *Relay* dengan *ESP32*

Relay Module	ESP32
VCC	5V
GND	GND
IN	26

Tabel 6. Koneksi *Buzzer* dengan *ESP32*

Buzzer	ESP32
GND	GND
Signal	27

Tabel 7. Koneksi *Solenoid Door Lock*

Solenoid	Koneksi
VCC	Relay Output
GND	Adaptor 12V

Tabel 8. Koneksi *ESP32-CAM* dan *ESP32*

ESP32-CAM	ESP32
GND	GND
13	27

Pengembangan perangkat lunak dilakukan melalui pemrograman arsitektur *dual-microcontroller* menggunakan *Arduino IDE* untuk menangani proses autentikasi, aktuasi, dan komunikasi data, serta pembangunan *backend* dan *frontend web server* menggunakan

Node.js, *Express JS*, dan *React JS* dengan *MySQL* sebagai basis data.

3.3.2. Proses Testing

Pengujian dilakukan menggunakan metode *Black Box Testing* secara bertahap per komponen hingga sistem terintegrasi secara keseluruhan. Skenario pengujian dibagi menjadi dua kelompok, pengujian perangkat *IoT* (8 skenario) dan pengujian antarmuka *web server* (8 skenario). Selain itu, dilakukan pengujian penerimaan pengguna melalui *UAT* yang melibatkan 30 responden terdiri dari 14 pengurus dan 16 anggota aktif LPM UNSIKA, dipilih menggunakan teknik *purposive sampling* berdasarkan kriteria keterlibatan langsung dengan sistem.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Perancangan Perangkat Keras

Sistem dirancang menggunakan arsitektur dual-microcontroller dengan komponen utama yang ditunjukkan pada Tabel 9.

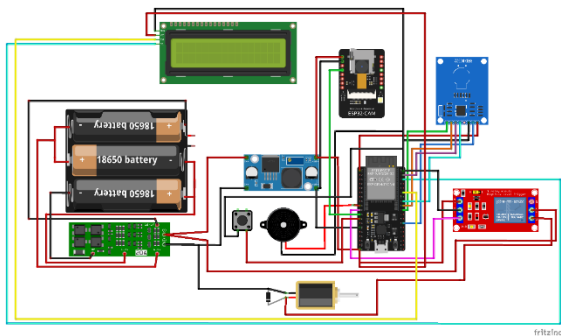
Tabel 9. Alat Yang Dibutuhkan

No	Komponen	Fungsi
1	ESP32	ESP32 berfungsi sebagai mikrokontroler utama yang mengontrol seluruh proses pada sistem. Perangkat ini membaca data dari RFID reader, memproses autentikasi pengguna, serta mengirimkan data aktivitas akses ke server melalui jaringan Wi-Fi.
2	RFID Reader MFRC522	RFID Reader MFRC522 berfungsi untuk membaca kartu atau tag RFID yang digunakan sebagai identitas pengguna. Ketika kartu RFID didekatkan ke reader, sistem akan membaca UID kartu untuk dilakukan proses verifikasi.
3	Kartu RFID	Kartu RFID berfungsi sebagai media autentikasi pengguna yang digunakan untuk membuka pintu. Setiap

		kartu memiliki UID unik yang akan didaftarkan pada sistem.
4	Solenoid Door Lock	Solenoid door lock berfungsi sebagai pengunci pintu otomatis yang akan terbuka ketika sistem memberikan sinyal dari mikrokontroler setelah kartu RFID terverifikasi.
5	Relay Module	Relay digunakan sebagai saklar elektronik yang berfungsi untuk mengontrol aliran listrik ke solenoid door lock yang membutuhkan tegangan lebih tinggi dibandingkan mikrokontroler.
6	LCD 16x2 I2C	LCD digunakan untuk menampilkan informasi kepada pengguna, seperti status akses berhasil atau ditolak setelah proses autentikasi RFID dilakukan.
7	Buzzer	Buzzer berfungsi sebagai indikator suara yang memberikan notifikasi ketika akses diterima maupun ketika akses ditolak.
8	Kamera OV2640	Kamera OV2640 digunakan untuk mengambil gambar ketika pengguna melakukan proses akses ke pintu sebagai dokumentasi tambahan dalam sistem monitoring.
9	Kabel Jumper	Kabel jumper digunakan untuk menghubungkan berbagai komponen elektronik pada rangkaian sistem selama proses perancangan dan pengujian alat.
10	Breadboard	Breadboard digunakan sebagai media perakitan

rangkaian sementara yang memudahkan proses pengujian dan pengembangan sistem sebelum dilakukan pemasangan permanen.

Perakitan seluruh komponen mengacu pada wiring diagram yang ditunjukkan pada Gambar 4. ESP32 sebagai pengontrol utama terhubung dengan modul *RFID MFRC522* melalui antarmuka *SPI*, modul *relay* untuk mengendalikan *solenoid door lock* 12V, *LCD 16x2* melalui protokol *I²C*, serta *buzzer* sebagai indikator suara. *ESP32-CAM* terhubung dengan kamera *OV2640* dan menerima sinyal *trigger* dari *ESP32* utama melalui pin *GPIO* untuk mengeksekusi pengambilan foto secara *event-driven*.



Gambar 4. Wiring Diagram Sistem

Hasil perakitan fisik sistem ditunjukkan pada Gambar 5 dan Gambar 6, di mana seluruh komponen ditempatkan di dalam box akrilik sebagai media *mounting* dan dipasang langsung pada pintu Ruang Redaksi LPM UNSIKA.



Gambar 5. Tampilan Depan Alat

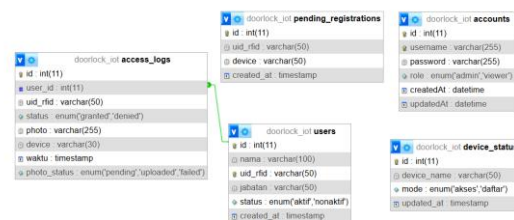


Gambar 6. Tampilan Belakang Alat

4.2. Hasil Perancangan Perangkat Lunak

4.2.1. Struktur Basis Data

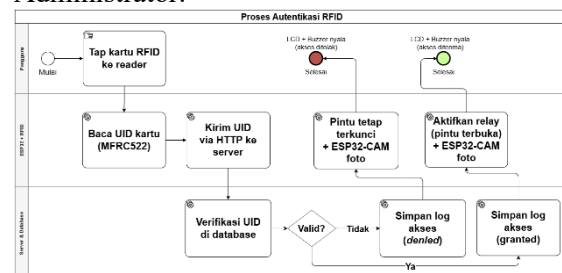
Basis data dirancang menggunakan *MySQL* dengan struktur yang ditunjukkan pada Gambar 7. Basis data menyimpan data kartu *RFID* terdaftar beserta identitas pengguna, riwayat seluruh aktivitas akses mencakup *UID*, waktu, status autentikasi, dan path foto hasil tangkapan *ESP32-CAM*, serta data akun pengguna antarmuka web beserta role masing-masing.



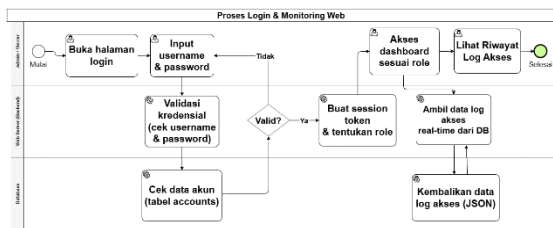
Gambar 7. Struktur Database Sistem

4.2.2. Pemodelan Proses Bisnis

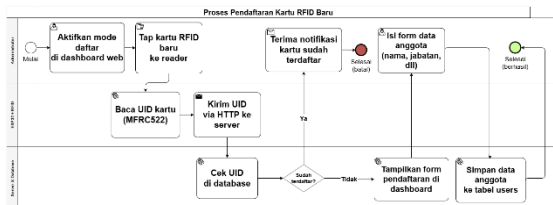
Alur proses sistem dimodelkan menggunakan *BPMN* yang ditunjukkan pada Gambar 8, Gambar 9, dan Gambar 10. Gambar 8 menggambarkan proses autentikasi *RFID* dari pemindaian kartu hingga eksekusi aktuasi pintu dan pencatatan log. Gambar 9 menggambarkan proses *login* dan monitoring melalui antarmuka *web*. Gambar 10 menggambarkan proses pendaftaran kartu *RFID* baru oleh Administrator.



Gambar 8. BPMN Autentikasi RFID



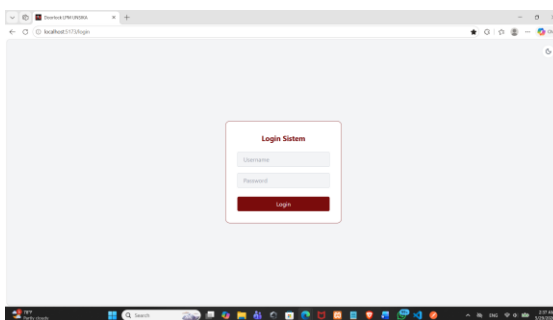
Gambar 9. BPMN Login & Monitoring Web



Gambar 10. BPMN Pendaftaran Kartu RFID Baru

4.2.3. Implementasi Antarmuka Web Server

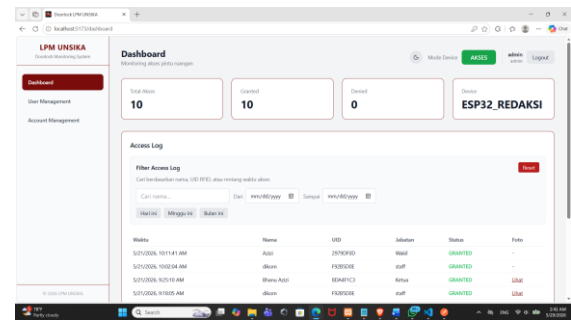
Antarmuka web dibangun menggunakan *React JS* pada sisi *frontend* dan *Express JS* pada sisi *backend*.



Gambar 11. Halaman Login

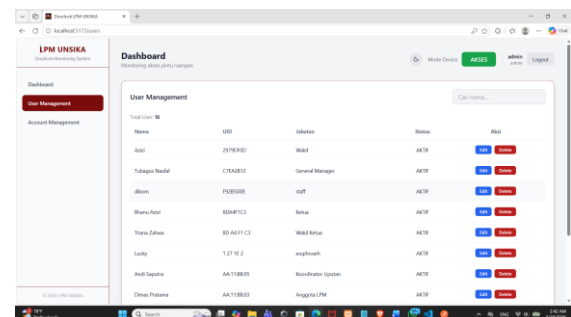
Gambar 11 menunjukkan halaman login yang berfungsi sebagai gerbang akses sistem bagi Administrator maupun Viewer.

Gambar 12 menunjukkan halaman dashboard yang menampilkan ringkasan total akses, jumlah akses diterima, dan jumlah akses ditolak secara *real-time*, dilengkapi tabel log akses kronologis beserta foto hasil tangkapan *ESP32-CAM*.



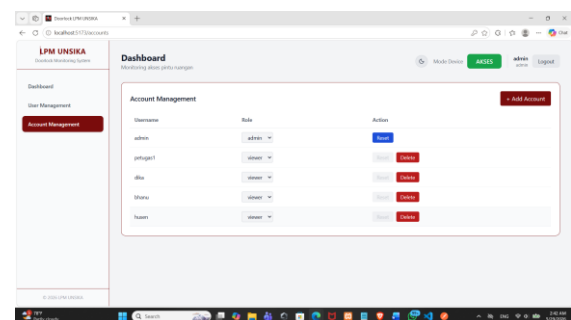
Gambar 12. Halaman Dashboard

Gambar 13 menunjukkan halaman user management untuk Administrator dalam mengelola data anggota dan kartu *RFID* terdaftar.



Gambar 13. Halaman User Management

Gambar 14 menunjukkan halaman account management untuk mengelola akun pengguna antarmuka web beserta pembagian role.



Gambar 14. Halaman Account Management

4.3. Hasil Pengujian Black Box Testing Perangkat IoT

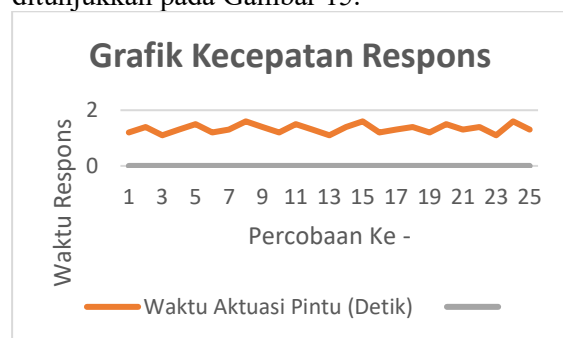
Pengujian fungsionalitas perangkat keras *IoT* dilakukan terhadap 8 skenario parameter utama. Hasil pengujian dirangkum pada Tabel 10.

Tabel 10. Hasil Pengujian Black Box Perangkat IoT

No	Skenario Pengujian		Hasil Uji	Kesimpulan
1	Supply Test	Power	Sesuai	Valid
2	Wi-Fi Connection Test		Sesuai	Valid
3	RFID Authentication Test		Sesuai	Valid
4	Solenoid Lock Test	Door	Sesuai	Valid
5	Buzzer Test		Sesuai	Valid
6	LCD Test		Sesuai	Valid
7	Camera Capture Test		Sesuai	Valid
8	Data Transmission Test		Sesuai	Valid

Berdasarkan Tabel 10, seluruh 8 skenario pengujian perangkat *IoT* dinyatakan valid. Sensor *RFID MFRC522* terbukti mampu membaca kartu secara akurat pada jarak 0–3 cm dengan waktu transmisi data ke server rata-rata di bawah 2 detik pada kondisi jaringan stabil. *Solenoid door lock* membuka pintu selama 3 detik setelah akses diterima kemudian mengunci kembali secara otomatis. *ESP32-CAM* berhasil mengambil dan mengirimkan foto ke *server* pada setiap pemindaian kartu, meskipun kualitas foto menurun pada kondisi pencahayaan rendah sebagai keterbatasan teknis sensor *OV2640* yang perlu diperhatikan pada pengembangan lanjutan.

Selain pengujian fungsional, dilakukan pengujian kecepatan respons sistem sebanyak 25 percobaan untuk mengukur waktu aktuasi pintu dari pemindaian kartu *RFID* hingga solenoid door lock merespons. Hasil pengujian ditunjukkan pada Gambar 15.

**Gambar 15.** Grafik Kecepatan Respons

Berdasarkan Gambar 15, waktu aktuasi pintu berkisar antara 1,1 hingga 1,6 detik

dengan nilai rata-rata 1,32 detik. Seluruh 25 percobaan menghasilkan waktu respons di bawah 2 detik, membuktikan bahwa sistem mampu memberikan respons aktuasi secara konsisten. Variasi waktu yang terjadi dipengaruhi oleh kondisi jaringan *Wi-Fi* lokal pada saat pengujian berlangsung, namun tidak berdampak signifikan terhadap performa keseluruhan sistem.

4.4. Hasil Pengujian Black Box Testing Web Server

Pengujian fungsionalitas antarmuka web server dilakukan terhadap 8 skenario operasional. Hasil pengujian dirangkum pada Tabel 11.

Tabel 11. Hasil Pengujian Black Box Web Server

No	Skenario Pengujian	Hasil Uji	Kesimpulan
1	Login Test	Sesuai	Valid
2	Wrong Credential Test	Sesuai	Valid
3	Role Restriction Test	Sesuai	Valid
4	Monitoring Log Akses Test	Sesuai	Valid
5	RFID Registration Test	Sesuai	Valid
6	RFID Management Test	Sesuai	Valid
7	Account Management Test	Sesuai	Valid
8	Real-time Update Test	Sesuai	Valid

Berdasarkan Tabel 11, seluruh 8 skenario pengujian antarmuka *web server* dinyatakan valid. Sistem autentikasi *login* berjalan dengan pembatasan hak akses yang benar antara Administrator dan Viewer, di mana Administrator diarahkan ke dashboard dengan akses penuh sedangkan Viewer memperoleh akses terbatas pada halaman monitoring. Sistem menampilkan pesan kesalahan yang sesuai pada percobaan login dengan kredensial tidak valid tanpa memberikan informasi spesifik mengenai field mana yang salah, untuk menjaga keamanan. Data log akses yang dikirimkan perangkat *IoT* berhasil ditampilkan secara akurat dan diperbarui secara real-time tanpa memerlukan pemuatan ulang halaman. Perubahan data kartu *RFID* yang dilakukan

melalui dashboard langsung dikenali oleh perangkat keras pada autentikasi berikutnya, membuktikan integrasi yang erat antara komponen perangkat lunak dan perangkat keras dalam ekosistem *IoT* yang dibangun.

4.5. Hasil User Acceptance Testing (UAT)

Pengujian *UAT* melibatkan 30 responden terdiri dari 14 pengurus dan 16 anggota aktif LPM UNSIKA menggunakan teknik purposive sampling. Setiap responden mengisi kuesioner 12 pernyataan yang dikelompokkan dalam empat aspek penilaian. Hasil rekapitulasi ditunjukkan pada Tabel 12.

Tabel 12. Rekapitulasi Persentase Penerimaan Pengguna per Aspek UAT

No	Aspek & Pernyataan	Skor Diperoleh	Skor Maksimum	Persentase
A	Kemudahan Penggunaan Sistem			92,00%
1	Kemudahan penggunaan RFID	137	150	91,33%
2	Kemudahan memahami LCD	141	150	94,00%
3	Kemudahan antarmuka Web Server	136	150	90,67%
B	Kemampuan Sistem Menyelesaikan Kebutuhan			94,22%
4	Keberhasilan verifikasi kartu	144	150	96,00%
5	Keakuratan catatan riwayat	143	150	95,33%
6	Efektivitas kamera dokumentasi	137	150	91,33%
C	Kenyamanan Penggunaan			92,00%

	Perangkat IoT			
7	Kecepatan respon sistem	134	150	89,33%
8	Manfaat indikator suara (buzzer)	139	150	92,67%
9	Kenyamanan aktivitas sehari-hari	141	150	94,00%
D	Kepuasan Pengguna Secara Keseluruhan			94,22%
10	Kepraktisan dibanding kunci fisik	139	150	92,67%
11	Kepuasan kinerja keseluruhan	142	150	94,67%
12	Kesediaan penggunaan rutin	143	150	95,33%
TOTAL KESELURUHAN		1676	1800	93,11%

Berdasarkan Tabel 12, seluruh responden memberikan penilaian pada kategori Setuju dan Sangat Setuju tanpa ada yang memberikan skor Netral, Tidak Setuju, maupun Sangat Tidak Setuju. Aspek Kemampuan Sistem dan Kepuasan Keseluruhan meraih persentase tertinggi sebesar 94,22%, dengan indikator keberhasilan verifikasi kartu *RFID* menjadi yang tertinggi sebesar 96,00%. Secara kumulatif sistem mencapai rata-rata 93,11% kategori Sangat Baik, sehingga layak diimplementasikan secara permanen di Ruang Redaksi LPM UNSIKA.

4.6. Pembahasan

Hasil penelitian ini menunjukkan bahwa sistem kunci pintu otomatis berbasis *IoT* dengan autentikasi *RFID* dan monitoring akses melalui *web server* berhasil dirancang, diimplementasikan, dan diuji secara langsung di Ruang Redaksi LPM UNSIKA. Dibandingkan dengan penelitian terdahulu, penelitian ini

memiliki kebaruan yang belum ditemukan secara bersamaan pada penelitian sebelumnya.

Nurwijayanti dan Basyir [5] serta Fathiah dkk. [6] hanya mengandalkan autentikasi RFID tanpa bukti visual, sehingga tidak dapat membuktikan apakah kartu digunakan oleh pemilik yang sah. Penelitian ini mengatasi keterbatasan tersebut dengan mengintegrasikan *ESP32-CAM* yang secara otomatis mengambil foto pada setiap pemindaian kartu, baik akses diterima maupun ditolak, sehingga menghasilkan audit trail visual yang lengkap. Candra dan Elvantio [9] telah mengintegrasikan dokumentasi foto berbasis *IoT*, namun belum menyediakan penyimpanan historis yang terstruktur dan dapat dikelola dari jarak jauh. Penelitian ini melengkapi hal tersebut dengan menyediakan *web server* yang menyajikan log akses secara real-time beserta foto bukti yang dapat dikelola Administrator dari jarak jauh tanpa pemrograman ulang perangkat keras.

Keunggulan utama sistem ini terletak pada dua aspek yang bekerja secara sinergis: pertama, histori penggunaan ruangan yang lengkap karena setiap aktivitas akses tercatat beserta identitas pengguna, waktu, status validitas, dan bukti foto secara otomatis ke dalam basis data; kedua, kemampuan deteksi penyalahgunaan akses karena dokumentasi visual memungkinkan administrator mengidentifikasi apakah kartu *RFID* digunakan oleh pemilik yang sah atau dipinjamkan kepada pihak yang tidak berwenang.

Meskipun demikian, sistem ini masih memiliki beberapa keterbatasan. Pertama, kualitas foto *ESP32-CAM* menurun pada kondisi pencahayaan rendah akibat keterbatasan teknis sensor *OV2640*. Kedua, sistem memiliki ketergantungan penuh terhadap stabilitas jaringan *Wi-Fi* lokal karena seluruh logika validasi diproses di sisi *server*, sehingga apabila koneksi terputus, proses verifikasi tidak dapat berjalan. Ketiga, terdapat ketidakkonsistenan penyimpanan data log akses pada sesi pengujian yang disebabkan oleh ketidakstabilan koneksi jaringan. Keterbatasan-keterbatasan ini dapat diatasi pada pengembangan lanjutan dengan penambahan penyimpanan lokal menggunakan modul SD card, pencahayaan eksternal di area pemindaian, serta fitur notifikasi *real-time* melalui bot Telegram atau WhatsApp untuk

percobaan akses menggunakan kartu tidak terdaftar.

5. KESIMPULAN

- Sistem kunci pintu otomatis berbasis *IoT* berhasil dirancang dan diimplementasikan pada Ruang Redaksi LPM UNSIKA menggunakan *ESP32* sebagai mikrokontroler utama yang mengoordinasikan sensor *RFID MFRC522*, *solenoid door lock*, modul *ESP32-CAM*, *LCD 16x2*, dan *buzzer*. Sistem terbukti mampu memverifikasi kartu *RFID* secara akurat pada jarak 0–3 cm dengan waktu respons aktuasi pintu rata-rata 1,32 detik dan seluruh 25 percobaan menghasilkan waktu di bawah 2 detik. Hasil *Black Box Testing* terhadap 16 skenario pengujian seluruhnya dinyatakan valid, dan *User Acceptance Testing* menghasilkan rata-rata persentase penerimaan sebesar 93,11% yang tergolong kategori Sangat Baik.
- Sistem berhasil terintegrasi secara utuh dengan *web server* sebagai komponen monitoring pendukung yang bekerja secara *real-time*. Melalui integrasi protokol *HTTP*, *web server* mampu mengelola basis data kartu *RFID* secara terpusat dan menyajikan data aktivitas akses secara akurat, mencakup identitas pengguna, waktu akses, status autentikasi, dan bukti foto hasil tangkapan *ESP32-CAM*. Sinkronisasi ini memungkinkan Administrator melakukan pengelolaan otorisasi kartu dari jarak jauh tanpa pemrograman ulang pada perangkat keras di lapangan.
- Kebaruan penelitian ini dibandingkan penelitian sebelumnya terletak pada kombinasi autentikasi *RFID* dengan dokumentasi visual otomatis dan monitoring terpusat berbasis web dalam satu sistem terintegrasi, sehingga sistem tidak hanya berfungsi sebagai pengunci otomatis tetapi juga sebagai alat deteksi dan investigasi penyalahgunaan akses ruangan secara menyeluruh.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Purwantoro, M.Kom. dan Ibu Susilawati, M.Si. selaku dosen pembimbing yang telah memberikan bimbingan, masukan, dan arahan selama proses penelitian

berlangsung. Penulis juga mengucapkan terima kasih kepada seluruh pengurus dan anggota Lembaga Pers Mahasiswa (LPM) UNSIKA yang telah bersedia menjadi responden dan memberikan kemudahan akses selama proses penelitian, serta kepada Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang atas dukungan fasilitas dan akademik yang diberikan.

DAFTAR PUSTAKA

- [1] D. Al Hafizd, A. Asnawi, dan M. A. Fikri, "Kajian Kebijakan Keamanan Sistem Informasi Sebagai Bentuk Perlindungan Kerahasiaan Pribadi Karyawan Perusahaan BFI Finance," *Jurnal Jurnal Sains Dan Teknologi (JSIT)*, 2023.
- [2] M. Puji Putra Pratama dan H. Adianto, "Alat Keamanan Menggunakan Sensor Gerak Dengan ESP32 Cam Berbasis Iot," 2023. [Daring]. Tersedia pada: <http://jurnal.bsi.ac.id/index.php/insantek>
- [3] S. Sendari dkk., "Penerapan Kartu RFID Berbasis Internet Of Things untuk Efisiensi Pelacakan Peralatan Laboratorium di Sekolah Kejuruan," *Jurnal Abdimas Berdaya*, 2023.
- [4] M. S. Z. M. Zabidi dkk., "IoT RFID Lock Door Security System," dalam *Journal of Physics: Conference Series*, Institute of Physics, 2022. doi: 10.1088/1742-6596/2312/1/012092.
- [5] K. N. Nurwijayanti dan A. Basyir, "PERANCANGAN SISTEM KEAMANAN PINTU RUANGAN OTOMATIS MENGGUNAKAN RFID BERBASIS INTERNET OF THINGS (IoT)," *Jurnal Ilmiah MATRIK*, vol. 24, no. 1, 2022.
- [6] Fathiah, H. Maulana, Baihaqi, dan Mursyidin, "PERANCANGAN SMART DOOR LOCK BERBASIS RFID DAN KEYPAD," *Jurnal Pendidikan Teknologi informasi*, vol. 8, no. 2, hlm. 80–88, 2024.
- [7] D. Aulia Ramadini dan Hastuti, "SISTEM KUNCI ELEKTRONIK PINTU KOS MENGGUNAKAN IOT BERBASIS E-KTP," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 1, hlm. 2830–7062, 2025, doi: 10.23960/jitet.v13i1.6177.
- [8] J. Jardian, Kevin, dan Michael Owen, "Perancangan Smart Door Berbasis ESP32-WROVER dengan Sistem Notifikasi Melalui Aplikasi Blynk," *Telcomatics*, vol. 9, no. 2, hlm. 40–46, Des 2024, doi: 10.37253/telcomatics.v9i2.10096.
- [9] R. Candra dan Z. Elvantio, "Pembuka Kunci Pintu Ruang Isolasi Mandiri Menggunakan Suhu Tubuh Dengan Notifikasi Foto Menggunakan Konsep IoT," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 12, no. 1, hlm. 93–98, Feb 2025, doi: 10.25126/jtiik.2025128759.
- [10] F. Humam dan M. A. Triawan, "Sistem Keamanan Ruangan Menggunakan ESP32CAM dan Sensor Gerak Berbasis IoT," *Infotek: Jurnal Informatika dan Teknologi*, vol. 7, no. 2, hlm. 575–584, Jul 2024, doi: 10.29408/jit.v7i2.26109.
- [11] A. Akbar, Zaenudin, Z. Mutaqin, dan L. D. Samsumar, "IoT-Based Smart Room Using Web Server-Based Esp32 Microcontroller," *Formosa Journal of Computer and Information Science*, vol. 1, no. 2, Des 2022, doi: 10.55927/fjicis.v1i2.1151.
- [12] W. W. Anggoro dan I. R. Widiyari, "Perancangan dan Penerapan Kendali Lampu Ruangan Berbasis IoT (Internet of Things) Android," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, no. 3, 2021, [Daring]. Tersedia pada: <http://jurnal.mdp.ac.id>
- [13] F. Abdaoe, H. Setiawan, M. Kom, dan K. S. T. Perdana, "Sistem Kendali Lampu Otomatis Berbasis Iot (Internet Of Things) Menggunakan Nodenum," *Bangkit Indonesia*, vol. IX, no. 01, 2021.
- [14] L. Sufra Alfarizi, A. Dwi Septiadi, dan K. Indartono, "Pemanfaatan Teknologi Radio Frequency Identification (RFID)," *Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK*, vol. 14, no. 2, 2020.
- [15] T. Oktovialenta, "RANCANG BANGUN PURWARUPA SMART ATTENDANCE SYSTEM BERBASIS TEKNOLOGI INTERNET OF THINGS (IoT)," 2025.
- [16] N. Dwi Setiawan, "ELKOM (Jurnal Elektronika dan Komputer) Rancang Bangun Sistem Real-Time Monitoring Suhu dan Kelembaban Menggunakan ESP32," *ELKOM (Jurnal Elektronika dan Komputer)*, vol. 18, no. 1, 2025, [Daring]. Tersedia pada: <https://journal.stekom.ac.id/index.php/elkom>
- [17] A. Rio Maldini, Herlinawati, E. Nasrullah, dan A. Sadnowo Repelianto, "Internet of Things dengan Modul NodeMCU ESP8266 V3 dan ESP32-CAM," *ELECTRICIAN – Jurnal Rekayasa dan Teknologi Elektro*, vol. 16, no. 2, 2022.
- [18] A. Hakim, Y. Lestiyanti, M. F. Asrori, N. Laela, dan A. Nurcholis, "Perancangan Smart Door Lock System dengan Multi Sensor untuk Sistem Keamanan Rumah," 2023.
- [19] T. Seda Mulya dkk., "RFID Untuk Sistem Keamanan Dan Pelacakan: Tinjauan Literatur (Tri Seda Mulya, Aisyah Aira Putri Maharani, Michael Steven, Diky Zakaria : Halaman 9-16) RFID Untuk Sistem Keamanan Dan Pelacakan: Tinjauan Literatur," 2025.

- [20] M. Ahmadar, P. Perwito, dan C. Taufik, "PERANCANGAN SISTEM INFORMASI PENJUALAN BERBASIS WEB PADA RAHAYU PHOTO COPY DENGAN DATABASE MySQL," *Dharmakarya*, vol. 10, no. 4, hlm. 284, Des 2021, doi: 10.24198/dharmakarya.v10i4.35873.
- [21] M. R. Nahjan, A. A. Ridha, N. Heryana, dan A. Voutama, "RANCANG BANGUN WEBSITE PENCARIAN INFORMASI BERITA DAN CUACA DAERAH DI INDONESIA MENGGUNAKAN API DAN EXPRESS.JS," 2023.
- [22] T. Sulistyorini, E. Sova, dan R. Ramadhan, "PEMANTAUAN KASUS PENYEBARAN COVID-19 BERBASIS WEBSITE MENGGUNAKAN FRAMEWORK REACT JS DAN API," vol. 1, no. 4, 2022, [Daring]. Tersedia pada: www.corona.jakarta.go.id.
- [23] Okpatrioka, "Research And Development (R&D) Penelitian Yang Inovatif Dalam Pendidikan," *DHARMA ACARIYA NUSANTARA : Jurnal Pendidikan, Bahasa dan Budaya*, 2023.
- [24] M. Waruwu, "Metode Penelitian dan Pengembangan (R&D): Konsep, Jenis, Tahapan dan Kelebihan," *Jurnal Ilmiah Profesi Pendidikan*, vol. 9, no. 2, hlm. 1220–1230, Mei 2024, doi: 10.29303/jipp.v9i2.2141.
- [25] N. Made, D. Febriyanti, A. A. Kompang, O. Sudana, dan N. Piarsa, "Implementasi Black Box Testing pada Sistem Informasi Manajemen Dosen," 2021.
- [26] M. A. Dava dkk., "Sistemasi: Jurnal Sistem Informasi Implementasi Website Bank Sampah menggunakan Pendekatan Agile Scrum dan User Acceptance Testing (UAT) Implementation of a Waste Bank Website using the Agile Scrum Approach and User Acceptance Testing (UAT)," *Sistemasi: Jurnal Sistem Informasi*, 2026, [Daring]. Tersedia pada: <http://sistemasi.ftik.unisi.ac.id>
- [27] H. Thabibi, S. F. A. Wati, dan T. P. Rinjeni, "Implementasi User Acceptance Testing (UAT) Pada Website E-Commerce UMKM BBhealthy," *Adopsi Teknologi dan Sistem Informasi (ATASI)*, vol. 4, no. 1, hlm. 19–26, Jun 2025, doi: 10.30872/atasi.v4i1.2904.
- [28] A. Aditya Santika, T. Hamonangan Saragih, D. Kartini, dan R. Ramadhani, "Penerapan Skala Likert Pada Klasifikasi Tingkat Kepuasan Pelanggan Agen BRILink Menggunakan Random Forest," *JUSTIN: Jurnal Sistem dan Teknologi Informasi*, vol. 11, no. 3, 2023, doi: 10.26418/justin.v11i3.